Amendments to the Claims

1. (currently amended) A Method for detecting fraud in a telecommunications system, the telecommunications system generating network event records, each network event record being generated in response to an event in the telecommunication system, the method comprising the steps of:

(1) performing ~~a plurality of types of~~ at least one fraud detection test[s] on the network event records;

(2) generating a fraud alarm[s] upon detection of suspected fraud by ~~any of~~ the at least one fraud detection test[s];

(3) correlating ~~the~~ fraud alarms ~~into fraud cases~~ based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and

(4) ~~automatically~~ responding to ~~certain of~~ the fraud case[s] with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

2. (new) The method of claim 1, wherein the method is performed by computer executable instructions disposed on at least one computer readable medium.

3. (new) The method of claim 2, wherein the computer executable instructions are distributed among a plurality of hardware platforms.

4. (new) The method of claim 2, wherein at least a portion of the computer executable instructions are implemented in a domain specific configuration.

5. (new) The method of claim 2, wherein at least a portion of the computer executable instructions are implemented in a core infrastructure.

6. (new) The method of claim 1, wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event record conforms to a predetermined format.

7. (new) The method of claim 1, wherein the at least one fraud detection test includes the step of enhancing the network event record such that an enhanced network event record includes data obtained from at least one external system.

8. (new) The method of claim 7, wherein the enhanced network event record includes data obtained from at least one database.

9. (new) The method of claim 8, wherein the at least one database includes at least one of a configuration database, an event database, a billing database, a call history database, and/or a records database.

10. (new) The method of claim 1, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a threshold rule, the alarm being generated if the network event record violates the threshold rule.

11. (new) The method of claim 10, wherein the alarm is generated if a value in the network event record exceeds a threshold value specified by the threshold rule.

12. (new) The method of claim 10, wherein the alarm is generated if a value in the network event record does not equal a value specified by the threshold rule.

13. (new) The method of claim 1, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a profile detection rule, the alarm being generated if the network event record violates the profile detection rule.

14. (new) The method of claim 13, wherein the network event record is compared to a normal usage profile.

15. (new) The method of claim 13, wherein the network event record is compared to a fraudulent usage profile.

16. (new) The method of claim 13, wherein the profile detection rule is based on historical network event records.

17. (new) The method of claim 1, wherein the at least one fraud detection test includes a comparison of at least a portion of the network event record to a predetermined pattern to identify a normal usage and/or a fraudulent usage.

18. (new) The method of claim 17, wherein the predetermined pattern is based on call history data.

19. (new) The method of claim 17, wherein the predetermined pattern is generated by a neural network.

20. (new) The method of claim 17, wherein the comparison is performed using tree-based algorithms that generate discrete output values.

21. (new) The method of claim 17, wherein the comparison is performed using statistical based algorithms that that employ iterative numerical processing techniques.

22. (new) The method of claim 1, wherein the step of correlating includes the step of enhancing a network event record by obtaining relevant data from an external source.

23. (new) The method of claim 1, wherein the step of correlating includes the step of applying at least one predetermined fraud analysis rule to the network event record to decide if a fraud case is appropriate.

24. (new) The method of claim 1, wherein the step of correlating includes the step of applying at least one predetermined prioritization rule to the fraud case to obtain the priority of the fraud case.

25. (new) The method of claim 1, wherein the fraud prevention action may be performed automatically, semi-automatically, or manually based on the priority.

26. (new) The method of claim 1, wherein the fraud prevention action is selected from a group that is comprised of at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification.

27. (new) The method of claim 1, wherein the alarm is selected from a group that is comprised of at least one of a long duration alarm, a call originating alarm, a call terminating alarm, a pin hacking alarm, a simultaneous calls alarm, a geographic alarm, and/or a call interval alarm.

28. (new) A system for monitoring one or more of a plurality of telecommunications networks, each of the plurality of telecommunications networks being characterized by a domain specific implementation, each telecommunications network being configured to generate network event records, each network event record being generated in response to an event occurring in the telecommunications network, the system comprising:

a fraud detection system including a core computing infrastructure and a domain specific infrastructure, the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored, the core computing infrastructure being non-domain specific, the fraud detection system being configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record.

29. (new) The system of claim 28, wherein the fraud detection system is dynamically reconfigured to adjust fraud detection rules in accordance with changing patterns of fraud.

30. The system of claim 28, wherein the fraud detection system further comprises:

a detection element coupled to the telecommunication system, the detection element being configured to generate a fraud alarm if the network event record is in violation of a predetermined fraud detection rule;

an analysis element configured to receive fraud alarms from the detection element, the analysis element being configured to correlate fraud alarms having common aspects, and generate a fraud case based on correlated fraud alarms; and an expert element coupled to the analysis element, the expert element being configured to apply at least one predetermined expert rule to assign a priority to the fraud case, the expert element performing a fraud prevention action in accordance with the priority.

31. (new) The system of claim 30, wherein the priority is based on a severity of suspected fraud.

32. (new) The system of claim 30, wherein the detection element includes at least one software processing engine comprising computer executable instructions disposed on at least one computer readable medium.

33. (new) The system of claim 32, wherein the at least one software processing engine is distributed among a plurality of hardware platforms.

34. (new) The system of claim 32, wherein the at least one software processing engine implemented in a domain specific configuration.

35. (new) The system of claim 32, wherein the at least one software processing engine includes a rules based thresholding engine configured to read the network event record and compare data in the network event record to a predetermined threshold.

36. (new) The system of claim 35, wherein the rules based thresholding engine further comprises:

at least one rules database;

a normalizer configured to configured the network event record in a standardized format;

an enhancer component coupled to the normalizer, the enhancer component being configured to insert additional data in the network event record; and

a threshold detector coupled to the enhancer component, the threshold detector being configured to compare the network event record to at least one threshold rule obtained from the at least one rules database, whereby the alarm is generated if the network event record violates the at least one threshold rule.

37. (new) The system of claim 36, wherein the enhancer component is coupled to an external systems interface, the additional data including data received from an external system.

38. (new) The system of claim 36, wherein the network event record includes an event key and at least one feature, the event key identifying the network event and the at least one feature including event measurement data.

39. (new) The system of claim 38, wherein the measurement data includes a count of a number of occurrences of an event during a predetermined time period.

40. (new) The system of claim 38, wherein the measurement data includes a count of a number of like events occurring simultaneously.

41. (new) The system of claim 38, wherein the measurement data includes geographic velocity data.

42. (new) The system of claim 36, wherein the at least one database comprises:

an enhancement rules database coupled to the enhancer component, the enhancer component obtaining an enhancement rule from the enhancement rules database based on data in the network event record; and

a threshold detection rules database coupled to the threshold detector, the threshold detector obtaining a threshold rule in accordance with data in the network event record.

43. The system of claim 42, wherein the enhancement rule directs the enhancer component to select external data from a selected external source.

44. (new) The system of claim 42, wherein the threshold rule stipulates that an alarm is generated when data in the network event record exceeds a threshold value.

45. (new) The system of claim 42, wherein the threshold rule stipulates that an alarm is generated when data in the network event record does not equal a threshold value.

46. (new) The system of claim 36, wherein the enhancer component provides the threshold detector with a feature vector, the feature vector including the event key and a plurality of feature event values, the event key including suspected fraud event identifying data, each feature event value of the plurality of feature event values providing fraud event measurement data.

47. (new) The system of claim 46, wherein the feature event value includes a threshold value.

48. (new) The system of claim 46, wherein the feature vector includes a name field, a value field, and a generating event field for each feature.

49. (new) The system of claim 48, wherein the feature vector is implemented as a data structure, the data structure being stored on a computer readable medium.

50. (new) The system of claim 48, wherein the feature vector includes at least one contributing event field for each feature.

51. (new) The system of claim 32, wherein the at least one software processing engine in the detection element further comprises:

a profiling database including at least one profile detection rule; and

a profiling engine configured to compare the network event record with at least one profile in accordance with the at least one profile detection rule, the profiling engine generating the alarm if the network event record substantially violates the profile detection rule.

52. (new) The system of claim 51, wherein the profile includes a normal use profile and/or a fraudulent use profile.

53. (new) The system of claim 51, wherein the profile is based on historical network event records.

54. (new) The system of claim 32, wherein the at least one software processing engine in the detection element comprises a pattern recognition engine configured to identify normal and/or fraudulent patterns of usage in the telecommunication network.

55. (new) The system of claim 54, wherein the pattern recognition engine compares the network event record to call history data obtained from a call history database.

56. (new) The system of claim 54, wherein the pattern recognition engine includes a neural network configured to identify fraudulent patterns of usage.

57. (new) The system of claim 54, wherein the pattern recognition engine includes tree-based algorithms.

58. (new) The system of claim 54, wherein the pattern recognition engine includes statistical based algorithms that that employ iterative numerical processing techniques.

59. (new) The system of claim 30, wherein the analysis element further comprises:

an external systems interface component configured to obtain data from external systems relevant to the fraud alarms;

a configuration database configured to specify any additional data required for fraud alarm analysis;

an alarm enhancement component coupled to the external systems interface and the configuration database, the alarm enhancement component being configured to add the additional data and external system data to the fraud alarm; and

a fraud case builder component coupled to the alarm enhancement component, the fraud case builder being configured to correlate and consolidate fraud alarms.

60. (new) The system of claim 59, wherein the fraud case builder is coupled to a rules database, the rules database providing the fraud case builder with parameters for generating fraud cases.

61. (new) The system of claim 30, wherein the expert element further comprises:

a configuration database configured to specify any additional data required for alarm analysis based on an alarm configuration;

an external systems interface component configured to obtain data from external systems relevant to at least one of the alarms;

a prioritizer component coupled to the configuration database and the external systems interface, the prioritizer being configured to direct the external system interface to obtain the additional data from at least one external system based on configuration data obtained from the configuration database, the prioritizer adding the additional data to the fraud case.

62. (new) The system of claim 61, wherein the prioritizer component receives prioritization rules from the configuration database and prioritizes the fraud cases in accordance with the prioritization rules.

63. (new) The system of claim 62, wherein the prioritization rules specify the fraud prevention action.

64. (new) The system of claim 63, further comprising an enforcement component coupled to the prioritizer component, the enforcement component performing the fraud prevention action based on the enhanced fraud case.

65. (new) The system of claim 30, wherein the fraud prevention action includes at least one of a card deactivation, a usage modification, an account deactivation, a range modification, and/or a privilege modification.

66. (new) The system of claim 30, wherein the alarm includes at least one of a long duration alarm, a call originating alarm, a call terminating alarm, a pin hacking alarm, a simultaneous calls alarm, a geographic alarm, and/or a call interval alarm.